ABSTRACT OF THE DISCLOSURE

Method and apparatus for protecting a firmware runtime environment are described herein. In one embodiment, a process example is provided to retrieve a first key from a secure store of a firmware within a platform, the firmware including an initialization table for initializing the platform, and verify the initialization table using the first key retrieved from the secure store during an initialization of the platform. Other methods and apparatuses are also described.